Remarks/ARGUMENTS

In response to the above-identified Final Office Action, Applicants have amended their application and respectfully request reconsideration thereof.

1. Summary of the Office Action

Claims 1, 2, 12, 14, 20, 21, 28, 32 and 33 stand rejected under 35 U.S.C. § 102(b) as being allegedly anticipated by Lei Tang entitled "Method for Encrypting and Decrypting MPEG Vide Data Efficiently" (hereinafter Tang). Claims 3-6, 13, 15-17, 19, 22, 23 and 25 stand rejected under 35 U.S.C. § 103(a), as being allegedly unpatentable over Lei Tang entitled "Method for Encrypting and Decrypting MPEG Video Data Efficiently" recited in the IDS, paper number 4 by Applicant, in view of U.S. Patent No. 6,567,533.

2. Claim Objections

The repeated phrase "for regenerating" has been removed from claims 15 and 16 in response to the objection stated in section 9 of the Final Office Action.

3. Response to § 102 and § 103 Rejections

Claims 1 and 12

As claims 1 and 12 essentially correspond in wording, insofar as the system for scrambling an information signal is concerned, these claims are discussed jointly in the following.

Claims 1 and 12 have been amended to clarify the subject-matter for which protection is sought, which is distinct from the disclosure in Tang, L., "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", *Proceedings of ACM Multimedia* '96, Boston, Nov. 18-22, pp. 219-229, hereinafter referred to - as in previous submissions - as Dl.

The amendments consist of the addition of the phrases 'information on' and 'received from the analysing means'. The first amendment is supported by the description page 8, line 10. As stated on page 8, line 38, the description at the top of page 8 applies to the use of the scrambling system described in general terms with reference to Fig. 1. Thus, there is sufficient information to infer that page 8, line 10 is applicable to the scrambling system in general, not just to embodiments for scrambling video signals. The second amendment is based on page 3, lines 15-16. Thus, the amendments to claims 1 and 12 do not extend the subject-matter of the present application unduly.

Novelty

Claims 1 and 12 are novel when compared with D1, because Dl does not disclose means for scrambling *the information signal* (i.e. the information signal of which the entropy distribution is analysed) in dependence on information on the entropy distribution of *the information signal*. Moreover, Dl does not disclose that the scrambling means provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of *the information signal.*

Instead, Dl discloses applying transform coding to video data represented as a set of images. The images are divided into macroblocks. A macroblock is composed of a set of 8 by 8 pixel blocks. The blocks arc transformed using the DCT. A permutation list with cardinality 64 is generated. A splitting procedure is comp1eted after the 8x8 is quantized. The random permutation list is applied to the split block, and the result is passed to an entropy coding procedure. This is explained in section 4.3 of Dl.

Suppose, for the sake of argument, that the video data prior to the DCT transform is to be regarded as the information signal. Then, clearly, the signal resulting from the DCT transform, the signal that is input to the scrambling process, hasn't a corresponding entropy distribution, particularly not after application of the 'splitting' procedure. Due to the 'splitting procedure' and permutations of the DCT coefficients, the 'probability distribution of run lengths is distorted' (page 226, right hand column, section 5). The signal resulting from application of the entropy coding procedure on the permuted DCT coefficients hasn't an entropy distribution corresponding to the pixel block before application of the DCT either.

Alternatively, if the DCT coefficients are to be regarded as the infomation signal, then their entropy distribution is not analysed in Dl, nor are they scrambled in dependence of the entropy distribution of the signal formed by them. Instead, the DCT

coefficients are subjected to the 'splitting procedure', then permuted in dependence on information in a permutation list unrelated to the entropy distribution of any signal, and then subjected to an entropy coding procedure. The 'splitting procedure' has the effect of smoothing the signal, so that the entropy component in the low-frequency range is increased. The permutation further changes the entropy distribution. Entropy coding results in a signal with increased high-frequency components.

Incidentally, it is observed that, were the Examiner to argue that the signal resulting from the entropy coding procedure is to be regarded as the scrambled information signal, so that the entropy coding procedure would be carried out by the scrambling means, then the known system fro scrambling the information signal would not comprise means for compressing the scrambled information signal. Thus this feature alone would distinguish the system of claim 1 from that known from Dl.

Therefore, the subject-matter of claim 1 is novel compared with Dl.

The subject-matter of claim 1 is also novel compared with US 6,567,533 Bl as set out in the submissions filed on May 12, 2004.

Obviousness

The subject-matter of claims 1 and 12 differs from Dl in that Dl does not disclose a scrambling system comprising means for scrambling the information signal (i.e. the information signal of which the entropy distribution is analysed) in dependence on information on the entropy distribution of the information signal received from the analysing means. Moreover, D1 does not disclose that the scrambling means provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal.

The effect of this difference is that, in the known system, at least part of the compression algorithm is carried out before scrambling (the DCT transform is carried out first, as is the 'splitting procedure'). Thus, it is not possible to apply existing compression and decompression techniques on the scrambled signal. This is conceded on page 220, left-hand column, penultimate paragraph. Furthermore, the known, adapted, compression algorithm is less effective, because the permuted and split DCT coefficients are less suited to the types of Variable Length Coding that are commonly comprised in means for compression of information signals. The objective problem solved by the present invention is to provide a system for scrambling an information

signal that allows effective compression of the scrambled information signal using existing compression techniques.

This problem is solved by providing the scrambling system with means for scrambling the information in dependence on the entropy distribution of the information signal received from the analysis means, to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal. Because the entropy distribution of the scrambled information signal corresponds to that of the information signal before scrambling, compression can be carried out just as effectively using existing compression tools.

The skilled person seeking to solve the problem identified above would not consult US 6,567,533 for its solution, as this document relates to methods for detecting unauthorised copies of information signals, not to preventing unauthorised copies. In particular, US 6,567,533 relates to a method for watermarking the information, signal, not to scrambling it. Thus, there is no reason or incentive for the skilled person to combine D1 with US 6,567,533. Even if the skilled person were to consult US 6,567,533, he would find only methods comprising steps of adding a signal to the information signal in such a manner that the entropy distribution of the signal is affected (column 18, lines 36-45).

The invention has the advantage of being particularly suited to protecting content information to be disseminated among users, such as video or audio information. There is no compressed descrambled information signal available to the user, so that unauthorised copying is made more difficult. Not only that, the provider of the unencrypted information signal can provide it at a certain bit rate in the knowledge that the scrambling process will not affect the demands on the capacity of the dissemination medium made by the compressed scrambled information signal; compression will be just as effective as it would be if carried out on the information signal prior to scrambling.

In summary, the combination of Dl and US 6,567,533 does not yield all technical features of claims 1 of 12. For these reasons, the subject-matter of claims 1 and 12 is not obvious having regard to the state of the art.

Claims 2-11, 13, 26, 28, 31-33

Claims 2-11 and 13 relate to systems for processing an information signal and a scrambling system according to claims 1 and 12, respectively. Because they are distinguished by the same novel and inventive features as the claims on which they are dependent, those claims also define subject-matter that is novel and not obvious. For the same reasons, claims 26, 28 and 31-33 relate to patentable inventions, because they relate to systems comprising all features of a system according to claim 12.

Claim 14

Claim 14 has been amended by specifying that it relates to a system for descrambling a scrambled information signal obtainable by combining a scrambling signal with the information signal. Basis for this amendment is to be found in claim 2 of the application as filed.

Novelty

The subject-matter of claim 14 is novel over D1, because D1 does not disclose means for regenerating the scrambling signal as a descrambling signal and means for combining the descrambling and scrambled information signals to obtain an information signal obtainable by combination with a scrambling signal. In particular, section 3 of Dl ('Related Works') discloses a selective encryption method of which the basic idea is to encrypt only the I-frames of the MPEG video.

If one were to regard interleaving of I-, P- and B-frames as a form of combination, as the Examiner appears to do, then the scrambled information signal (the combination of clear P- and B-frames and scrambled I-frames) is obtainable by combination of an information signal consisting of the clear P- and B-frames and a scrambling signal, consisting of the scrambled I-frames. However, DI would then not disclose the feature 'means for combining the scrambled information signal and scrambling signal to obtain the information signal', because the result of combining the scrambled I-frames with the combination of clear B- and P- and encrypted I-frames would not be a signal consisting of the clear P and B frames.

Therefore, the subject-matter of claim 14 is novel compared with Dl.

The subject-matter of claim 14 is also novel compared with US 6,567,533. Reference is made to the submissions filed on May 12, 2004, in this respect.

Obviousness

The subject-matter of claim 14 is not obviously derivable from the cited prior art either.

The descrambling system according to claim 14 differs from the one disclosed under 'Related Works' in Dl, in that the relevant passage of Dl does not disclose a descrambling system comprising means for regenerating the scrambling signal as a descrambling signal and means for combining the descrambling and scrambled information signals to obtain an information signal obtainable by combination with a scrambling signal.

The effect of the means for regenerating the scrambling signal as a descrambling signal and means for combining the descrambling and scrambled information signals to obtain an information signal obtainable by combination with a scrambling signal is that it is possible to add a large amount of variation into the scrambling process, making the scrambled information signal harder to 'crack'. Because the descrambling system comprises means for regenerating the scrambling signal, it is not necessary to provide a recording of the scrambling signal. Thus, the objective problem solved by the invention defined in claim 14, is to provide a descrambling system that allows a more secure scrambling of the information signal as well as efficient dissemination of the scrambled information signal and key information.

The other descrambling system disclosed in Dl would not be considered as offering a solution to this problem, because it requires communication of a permutation vector to undo the permutation of DCT coefficients, which permutation vector must be communicated to the descrambling system. Because the scrambled information signal is not obtainable by combination of the information signal with a scrambling signal, the other embodiment in Dl is not relevant to the objective technical problem to be solved. Even if it was relevant, then the means for undoing the permutation of DCT coefficients are not means for combining a descrambling signal and scrambled information signal. Thus, no combination of embodiments disclosed in Dl would yield a descrambling system as defined in claim 14.

US 6,567,533 does not relate to scrambling information signals or descrambling scrambled information signals, but to watermarking information signals. Therefore the

skilled person would have no motivation or incentive to apply any teaching of US 6,567,533 to the problem of providing a descrambling system that allows a more secure scrambling of the information signal as well as efficient dissemination of the scrambled information signal and key information. Moreover, the combination of Dl and US 6,567,533 does not yield all technical features of claim 14, as US 6,567,533 does not disclose means for combining a descrambling signal and scrambled information signal to obtain the information signal.

For these reasons, and because the descrambling system defined in claim 14 provides an effect not obtainable using the prior art techniques, the subject-matter of claim 14 is not obvious.

Claims 15-25 and 30

Claims 15-25 and 30 relate to systems having all features of a system according to claim 14. They thus also relate to patentable inventions.

In summary, Applicants believe that all rejections presented in the Final Office Action have been fully addressed and withdrawn of these rejections is respectfully requested. Applicants furthermore believe that all claims are now in a condition for allowance, which is earnestly solicited.

If there are any additional charges, please charge Deposit Account No. 02-2666. If a telephone interview would in any way expedite the prosecution of the present application, the Examiner is invited to contact Mark Vatuone at (408) 947-8200.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 10/1, 2004

Mark R. Vatuone
Reg. No. 53,719

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 947-8200